114th CONGRESS
2nd Session

Printed for the use of the
Commission on Security and Cooperation in Europe

INTERNET FREEDOM IN THE AGE OF DICTATORS AND TERRORISTS

MARCH 3, 2016

**Briefing of the
Commission on Security and Cooperation in Europe**

Washington: 2016

Commission on Security and Cooperation in Europe
234 Ford House Office Building
Washington, DC 20515
202–225–1901
csce@mail.house.gov
http://www.csce.gov
@HelsinkiComm

Legislative Branch Commissioners

HOUSE
CHRISTOPHER H. SMITH, NEW JERSEY
Chairman
ALCEE L. HASTINGS, FLORIDA
ROBERT B. ADERHOLT, ALABAMA
MICHAEL C. BURGESS, TEXAS
STEVE COHEN, TENNESSEE
ALAN GRAYSON, FLORIDA
RANDY HULTGREN, ILLINOIS
JOSEPH R. PITTS, PENNSYLVANIA
LOUISE MCINTOSH SLAUGHTER,
NEW YORK

SENATE
ROGER WICKER, MISSISSIPPI,
Co-Chairman
BENJAMIN L. CARDIN. MARYLAND
JOHN BOOZMAN, ARKANSAS
RICHARD BURR, NORTH CAROLINA
JEANNE SHAHEEN, NEW HAMPSHIRE
TOM UDALL, NEW MEXICO
SHELDON WHITEHOUSE, RHODE ISLAND

Executive Branch Commissioners

DEPARTMENT OF STATE
DEPARTMENT OF DEFENSE
DEPARTMENT OF COMMERCE

ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe (OSCE). The membership of the OSCE has expanded to 56 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <www.osce.org>.

ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is a U.S. Government agency created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <www.csce.gov>.

INTERNET FREEDOM IN THE AGE OF DICTATORS AND TERRORISTS

MARCH 3, 2016

COMMISSION STAFF PRESENT

Page

Shelly Heald Han, Policy Advisor for Economics, Environment, Technology and Trade, Commission on Security and Cooperation in Europe 1

PARTICIPANTS

Rebecca MacKinnon, Director, Ranking Digital Rights 2
Lisl Brunner, Director of Policy and Learning, Global Network Initiative 5
Tim Maurer, Associate, Carnegie Endowment for International Peace 8

APPENDIX

Prepared Statement of Lisl Brunner 25
Prepared Statement of Tim Maurer 29

INTERNET FREEDOM IN THE AGE OF DICTATORS AND TERRORISTS

MARCH 3, 2016

Commission on Security and Cooperation in Europe
Washington, DC

The briefing was held at 10 a.m. in room 2255, Rayburn House Office Building, Washington, DC, Shelly Heald Han, Policy Advisor for Economics, Environment, Technology and Trade, Commission on Security and Cooperation in Europe.

Panelists present: Rebecca MacKinnon, Director, Ranking Digital Rights; Lisl Brunner, Director of Policy and Learning, Global Network Initiative (GNI); and Tim Maurer, Associate, Carnegie Endowment for International Peace.

Ms. HAN. OK, it's 10:00 and we'll get started. Good morning, and welcome to the Commission on Security and Cooperation in Europe's briefing on Internet Freedom in the Age of Dictators and Terrorists.

About a decade ago, when the Internet was spreading like wildfire around the world, and Gmail, Facebook, and Twitter were taking off, I and a lot of other people jumped on the Internet freedom bandwagon, and hailed the Internet as a game changer for spreading democratic ideals to places that were closed off to traditional media and information. It was precisely because it was so powerful that the Internet moved into the crosshairs of governments because, to put it in simplistic terms, the autocrats fear that it can be used to usurp their power, and the democracies fear it because it might be used by criminals and terrorists.

Congressman Chris Smith, who's the chairman of our Commission in this Congress, first introduced the Global Online Freedom Act in 2007, in recognition of this threat to online users, particularly in closed societies, like China. And since 2007, we've seen the China model of Internet control spread throughout the world. And while several years ago, most of our fears about Internet freedom centered on foreign governments, in the post-Snowden world the debate has also shifted to what the U.S. Government is doing with our online information, the Apple versus FBI case being the most recent example.

Although it is often phrased as a privacy versus security issue, I think it is really a security versus security issue, particularly in the Apple case; the security of our online user information and the Internet infrastructure versus the overall security environment against terrorist threats. So the question becomes, again, a question that we've been asking a lot over the years, particularly since 9/11, is where do we draw the line? Should

we strive to know every bit of communication that passes between potential terrorists? And if so, at what cost?

So today, while I do want to talk about U.S. law enforcement demands, I think it is also just as important to remember that there are countries like China and Russia that have the technical capability and the political means to do much worse. Here in the United States we have the mechanism for a substantial political debate, public discussion, court cases, et cetera. Those options do not exist for the citizens of many, many other countries, where the Internet is both heavily censored and heavily surveilled.

So I'd like to turn to our panelists for their expert perspectives. First, we have Rebecca MacKinnon, who is the director of the Ranking Digital Rights Project which works to set global standards for how companies in the information and communications technology sector, and beyond, respect freedom of expression and privacy. She's also the author of this great book that I recommend to everyone, "The Consent of the Networked," which came out in 2012 and was really one of the first books to take a close look at the issue of users and their consent and what is happening online with that information. She currently serves on the board of directors of the Committee to Protect Journalists, and was a founding member of the Global Network Initiative.

Next, we'll hear from Lisl Brunner, who is responsible for GNI's policy development and learning program. Most recently, she was a facilitator for the telecommunications industry dialogue at GNI, where she coordinated a group of telecommunications operators and vendors, addressing freedom of expression and privacy rights in the context of the U.N. guiding principles on business and human rights.

And then finally, we'll have Tim Maurer, who's an associate at the Carnegie Endowment for International Peace. His work focuses on cyberspace and international affairs, with a concentration on global cybersecurity norms, human rights online, Internet governance, and their interlinkages. He is writing a book on cybersecurity and proxy actors. So we're particularly interested in how Tim addresses the export control issues that have been recently discussed in the news.

So, Rebecca, we'll start with you. Thank you.

Ms. MACKINNON. Thanks so much, Shelly. It's really great to be back here in the Rayburn Office Building to talk about Internet freedom. And I need to commend you, Shelly, who, I think, you along with some other members of Congress and staffers have been continuously and tirelessly calling attention to Internet freedom issues, and doing everything you can to keep these issues on the radar screen and in an institution that's dealing with an awful lot of things. [Laughs.] So I really commend you for your tireless work on these issues.

As you know, the Internet has obviously brought tremendous benefits to people, companies, economies all over the world. We've seen events in the past, particularly around the Arab Spring, but also at other points of time in a range of countries, where people have used social media and other network technologies to organize political movements and demand accountability of their governments. And this is obviously still a very important aspect.

Connectivity is growing fast according to the study by McKinsey on digital globalization and global data flows. Just think about this—the use of Internet bandwidth across borders has increased 45-fold since 2005. That's a lot. That's a lot of bandwidth that the Internet is burning, and that the cross-border connectivity of the Internet has

brought. And another, I think, really interesting statistic in that study, 900 million people around the world communicate with other people outside their countries on social media.

And obviously, for every type of reason imaginable—some that we would define as good, some that we would define as silly, and some that we would define as rather bad. That's been the subject of conversation at other hearings. But nonetheless, this interconnectivity and the role of companies in bringing people together is really important. Three hundred and sixty million around the world are taking part in cross-border e-commerce, not just e-commerce within their own borders. So the importance of this is that we need a globally interconnected Internet.

At the same time, in 2014, as Internet connectivity is growing, more than 213 million people around the world went online for the first time in 2014, most of them not in the West but in countries concentrated, in greatest numbers, India, Nigeria, South Africa, Russia, Egypt, Philippines. But what's really important to understand is that the massive increase in cross-border digital communication has not made the world more free in aggregate. And in fact, the Internet itself, in terms of people's ability to speak freely, to use it to organize, to use the Internet to carry out investigative journalism, is diminishing.

According to research by Freedom House, which produces the annual Freedom on the Net Index, which I recommend to you, new users have less freedom to speak their minds, freely access information, or organize around civil, and political, or religious interests. Even worse, according to their 2015 Freedom on the Net report, Internet freedom levels have declined steadily over the past five years, as they've examined the policies and practices of national governments around the world.

And there is a growing epidemic of laws that criminalize behavior online, also holding companies legally accountable for what their users are doing all over the world, and the passage of a growing number of cybercrime laws in countries where crime is defined to include activities critical to the government or investigative journalism. You're seeing more and more journalists being arrested on terrorism charges in a number of countries with the help, sometimes, of companies to track them down.

And Freedom House observed that a growing number of governments are not only censoring information in the public interest, but they're placing greater demands on the private sector to take down offending content and track users. Shelly mentioned China. And we have seen China sort of as the model for how this started over a decade ago. The Committee to Protect Journalists just came out with a report this morning detailing how one of China's major social media companies works with government authorities to censor and track users. And I suggest you go to CPJ.org to see that.

But an interesting thing to point out is that a decade ago, when people first started talking about Internet censorship and Internet freedom, everybody was focused on the blocking of websites, right? You know, Facebook is blocked in China and Twitter is blocked in China, and, there's a lot of what we call filtering or blocking. But that's only one layer of the story. What we're seeing in China is a very sophisticated collaboration between domestic companies and governments, saying, well, if you don't collaborate with us, we're going to block you.

So there is a sophisticated system of taking down content on platforms, not just blocking it at the Internet service level. And that type of practice has spread all over the world, in all kinds of political systems. It's certainly not limited to authoritarian countries like China. You know, a Russian woman was recently sentence to hard labor for reposting

on social media critiques of Russian actions in Ukraine. We're seeing a lot of blocking—not only blocking in Russia, but people being tracked down and arrested. And this is done with the help of the companies.

So we're seeing this trend—and it can feel quite depressing at times. But I do want to point to some positive things. Frankly, I think the situation would be a lot worse today if the major U.S. Internet companies that operate around the world had not stepped up and made some commitments to respect their users' freedom of expression and privacy, particularly in relation to government demands that they're getting. And we saw—and, again, I need to commend Shelly and a number of members of the House and Senate, and their staffers, for really shining a light on some of the problems that we were seeing with U.S. Internet companies operating around the world—the case of Shi Tao in China with Yahoo and so on, and really pushing companies to step up to the plate; and the formation of the Global Network Initiative in 2008 with Google, Yahoo, and Microsoft initially on board. And we now have Facebook hooked in, and, you know, some European telecommunications companies are joining as observers. And I think Lisl will talk about the details of the commitments that these companies are making, their commitment that they ought to make not only to certain principles but also to engage with human rights groups, to engage with other stakeholders, to advocate for better policies, and also to be assessed on whether they're actually carrying out their commitments.

But one of the problems is that only a small number of companies have actually stepped up. And we are seeing some companies—like, for instance, Apple is not a member of the Global Network Initiative. They stood up for their users on encryption, but there are a lot of questions about other things that they may or may not be doing, and how consistently they are adhering to their commitments in other markets, such as China.

That is one of the reasons I decided to start a new project that's really complementary to the Global Network Initiative, called Ranking Digital Rights. I have some materials outside about the corporate accountability report that we just released. But I felt we needed to compare more companies against one another, and how their policies and practices stack up, and also to get a sense of the extent to which GNI membership and the commitments through GNI are affecting companies' performance.

And one of the things we did find, in fact, is that GNI member companies are showing more consistent transparency, more consistent policy implementation around the world. Not that anybody's perfect, but particularly when it comes to human rights impact assessments to engaging with stakeholders in a consistent way, to institutionalizing commitments and showing evidence that they've institutionalized their practices across their companies, there's a real difference being made.

There's a much longer list of companies that are much more inconsistent. So I would point out for instance, just to make a couple of examples, again, Apple—you know, I commend them for what they're doing in response to U.S.Government demands recently. It's not clear whether they've ever carried out a human rights impact assessment on their business in China. And so I think, you know, with a company such as that, I would like to see them all be more consistent across the board.

Twitter has been standing up to a number of government demands around the world. They're very good on transparency reporting. But, again, to what extent have they institutionalized their practices? They themselves do not carry out human rights impact assessments. So there's some inconsistencies. AT&T, which has started to expand into Latin America, doesn't do human rights impact assessments. And so it would be, I think, good

to find a way to encourage more companies to step up alongside the small number of very powerful, but yet still limited, number of companies in the GNI.

I'm running out of time so I would just point out that we also have a broader problem that you spoke to, Shelly. We need governments around the world, particularly democratic governments, to step up and recognize that when you're regulating in your own jurisdiction there are global implications. There are global implications to the technology. There are global implications in terms of the legal frameworks you're putting in place.

We need to see clearer commitments from the United States, from Europe, from the governments that have joined the Freedom Online Coalition, which is part of the State Department's Internet Freedom Initiative, to really say: OK, yes, we need to fight terrorism, we need to fight crime, we need cybersecurity. But at the same time, we need to find out—we need to commit to a set of principles for how we're going to do this in a way that does not make it easier for repressive regimes to entrench their surveillance practices, to entrench the way—the legal mechanisms that they use to pressure companies to hand over user information, to privatize the censorship of discourse that is taking place around the world.

And right now, I think part of the problem we have is that we have a lot of urgent problems. And governments are kind of focusing on solving one problem without thinking about what are the broader international human rights impacts, what are the broader impacts on a globally free and open Internet? Because if we do not maintain a globally free and open Internet, if the human rights situation in developing, transitional countries becomes worse, in part because people cannot use technology to its full advantage, we're not going to be secure in the long run.

There's going to be more disenfranchised and disillusioned people out there on the planet. And so we really need to step up and say we care about protecting ourselves, but we care about the human beings on this planet, their security, their freedoms. And it is in our long-term interests to work towards that, both in terms of our policies and in terms of corporate commitment.

Ms. HAN. Thanks, Rebecca. That's a great way to start off the discussion. Lisl, do you want to go next?

Ms. BRUNNER. Sure. Thank you to Chairman Smith, to co-Chairman Wicker, to Shelly, and to the members of the Helsinki Commission for giving us the opportunity to provide an overview of the Global Network Initiative today, and some of its policy priorities. The Global Network Initiative, as Rebecca mentioned, is an international, multi-stakeholder collaboration between information and communications technology companies, civil society organizations, academics and investors. We were formed in 2008 and our mission is to promote human rights by creating a global standard for companies that supports responsible decisionmaking and by being a leading voice in policy debates to advance freedom of expression and privacy rights in the ICT sector.

Our company members include Facebook, Google, LinkedIn, Microsoft, and Yahoo. Non-company members include the Berkman Center for Internet & Society, Rebecca MacKinnon, Human Rights Watch, the Center for Democracy and Technology, Bolo Bhi in Pakistan, the Center for Internet & Society in India, and the Church of Sweden, among many others. We've also been collaborating over the past three years with companies participating in the telecommunications industry dialogue. And recently seven of those

global telecommunications companies became observers with the GNI, with a view to becoming full members next year. Those companies include Vodafone, Orange, and Nokia.

The GNI works in four areas. It provides a framework for responsible company decision making and action, it fosters accountability through company commitment to an independent assessment process to evaluate implementation principles, it promotes policy engagement, and it enables shared learning among our participants. In the first area, GNI's principles and implementation guidelines were developed through a multi-stakeholder process, and they're based on international human rights standards. Our guidelines are influenced by and are compatible with the U.N. guiding principles on business and human rights, and the protect, respect, and remedy framework. The GNI framework helps companies to respect and protect the freedom of expression and privacy rights of their customers and users when they respond to government demands, laws, and regulations. And companies worldwide can use this framework to implement their responsibility to respect human rights.

In terms of accountability, GNI members undergo a biannual assessment of their implementation principles, conducted by organizations that are accredited by the GNI's multi-stakeholder board, and which meet independence and competency criteria. In addition to reviewing the GNI members' policies and procedures, and interviewing its staff members, the assessor selects case studies which determine how the company has responded to government demands involving freedom of expression and privacy. The assessor then prepares a report which is reviewed by the GNI board, and the board determined whether the companies are complying with the companies. And this means that in the board's view, the company is making a good-faith effort to implement and to apply the GNI principles and to improve over time. In 2013, the GNI completed assessments for its three founding companies, and we're currently underway in our second round of assessments for all member companies. In terms of policy priorities, the GNI determines its policy priorities by identifying the challenges facing its member companies—both through its assessment process, and through its ordinary activities, and through the headlines, as you can imagine. The multi-stakeholder nature of the GNI gives us a deep capacity for informed and credible engagement with governments, intergovernmental organizations, and international institutions. And the GNI generally advocates for laws that are consistent with international human rights standards, and the principles of legality, necessity, and proportionality. At present, we're focusing our policy efforts on five issues of priority.

First, the GNI's concerned by the adoption of broad laws prohibiting extremist content and promotion of terrorism. The GNI acknowledges the legitimate national security and law enforcement obligations of governments, but at the same time there continues to be no internationally agreed-upon definition of terrorism. Across the world, counterterrorism laws have led to the criminalization of speech in political contexts and to the restrictions of large amount of content in places like Tajikistan. Similarly, some authorities have proposed that ICT companies should face criminal liability for failing to delete content praising terrorism from their platforms.

And this brings me to our second area of priority, which is legislation on intermediary liability and calls for service providers to police user content and communications, at times under broad and vague standards of which content is considered illegal.

Third, the GNI advocates for laws that regulate government access to user data in a way that protects the right to privacy. We have engaged with and provided input to

the U.K. government on its investigatory powers bill recently, for example. And the GNI has also urged governments to support strong encryption and not to subvert security standards.

Fourth, the GNI has advocated for reforms to the Mutual Legal Assistance regime, which is the dominant method for managing lawful government-to-government requests for data across jurisdictions. The regime has not been updated to keep track with the globalized data, which makes the process inefficient and opaque. And so requests to the U.S. Government take an average of 10 months to fulfill. As a result, authorities from other governments sometimes take drastic measures. These include demanding that their domestic laws apply extraterritorially, issuing mandates to localize data, and demanding the compromise of digital security of individuals. All of these measures would be harmful to an open, robust, and free Internet.

So the GNI had identified a series of practical and legal reforms that policymakers could adopt in order to reform the current mutual legal assistance regime. We also support efforts to develop a new international legal framework, which enables foreign law enforcement authorities to have efficient access to information, when this access is consistent with international norms and with the right to privacy. The GNI supports reforms that would allow governments to make requests for data from providers, as long as stringent human rights requirements apply and the process is characterized by robust transparency, accountability, and international credibility.

Fifth, the GNI has advocated for governments to take steps to be more transparent about the laws and legal interpretations that authorize electronic surveillance or content removal. And we urge governments and intergovernmental organizations to take a multistakeholder approach when they debate laws and policies that impact freedom of expression and privacy of global Internet users, and to ensure that these are subject to public debate.

Finally, in terms of learning, the GNI provides opportunities for its members to work through complex issues with other participants in a safe and confidential space. We've commissioned reports that examine challenges facing governments and technology companies as they balance their rights to freedom of expression and privacy with law enforcement and national security responsibilities. And we've held public learning forums to discuss these challenges in the United States, Brussels and Geneva.

I'll just conclude briefly with a few of our achievements. Through the GNI assessment process, we've seen improvements to company policies and procedures. We've seen more companies adopting and strengthening human rights impact assessments as part of the way that they do business. And we've seen enhanced company transparency with users and with the public at large. The implementation of the GNI principles has reduced the amount of content that has been removed and the amount of personal data that is released as a result of government requests around the world. And we've successfully encouraged governments to increase transparency and public debate on surveillance laws, and to improve their policies and practices in this regard. We've gotten commitments from Freedom Online Coalition member governments, and we've seen reforms of surveillance laws and intermediary liability laws around the world.

Thank you so much, and I'm happy to answer your questions.

Ms. HAN. Thanks, Lisl. Tim.

Mr. MAURER. Thank you, Shelly. And thanks to Chairman Smith, and Co-Chairman Wicker, and the members of the Commission for this opportunity to speak about the important role of export controls in the context of Internet freedom today.

In December 2013, the 41 member states of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies agreed to create two new controls focusing on cybersecurity items. The proposed implementation of these two controls by the U.S. Government last year sparked significant controversy, which touched on four dimensions that I think are important to consider: the growing empirical evidence of technology sold by companies in North America and Europe to customers and countries that use them to violate human rights; the benefit of these technologies for legitimate law enforcement and intelligence activities; the benefit of these technologies for cybersecurity, for example, to test and improve defenses; and the risks of these technologies for cybersecurity, for example, by providing more sophisticated hacking tools to actors who will use them for offensive purposes.

My remarks will focus on this first dimension, controlling exports of technologies that can be used to violate human rights in the context of Internet freedom, given the focus of this briefing. The controversy over the past year, and the significant pushback against the U.S. Government's proposed implementation of these new controls, are signs that the process that was used needs to be improved, in addition to the substantial challenges of implementing the new controls. Only two days ago, Secretary Pritzker announced in a letter that the U.S. Government will go back to Wassenaar to propose eliminating part of the language of the two new controls. Secretary Pritzker's letter is laudable for saying that the U.S. Government commits to engaging the public, getting the human rights community, industry, and the cybersecurity research community an opportunity to participate through the notice and comment process of the proposed rule.

So as we end this new phase, following Secretary Pritzker's letter, I'd like to offer the following observations and recommendations for moving forward. It is clear that addressing the underlying human rights problem that led to these new two controls can only be successful if they are coordinated multilaterally and if they're informed by technical analysis. U.S. leadership on this issue, and full investment in striking the right balance, can have a significant impact and help shape the standard internationally. One of the positive outcomes of the controversy of the past several months is the heightened awareness among all of the actors involved that the underlying human rights problem that led to the development of the new two controls has yet to be addressed. Export controls can be an effective tool to influence corporate behavior. The challenge is designing them in a way so that they only target the type of behavior deemed of concern, without affecting the rest.

Weighing these interests and weighing human rights and security concerns is not a novelty in the context of our export controls, especially in the context of DOD's technologies. However, this specific topic, and this new and growing industry, faces a limited amount of data, and therefore makes it much more difficult to find that right balance. So in terms of moving forward, I recommend focusing on the following two strategic priorities: increasing transparency and an efficient, and effective, and inclusive process.

There is a great need to increase the transparency in this field because one of the main challenges that we're all facing is that there is a lack of data, and there's a lack of data about the market, the products involved, and the trading. Greater transparency can be accomplished through voluntary action by company, but it can also be com-

plemented by the notification requirements of the export control issue, without necessarily imposing a licensing requirement. You can use this data to then review again the export control regime in a few years, and tailor it according to the data that you've received, and the better picture we will gain with regard to the market.

The second priority, on focusing on establishing an efficient and effective and inclusive process, is based on the controversy that we saw over the past year. The U.S. Government's decision to request public feedback is a promising sign to solicit input beyond the existing standing Technical Advisory Committees of the Department of Commerce. This is particularly important to reach communities such as the cybersecurity research community. The further improvement of this process could consist of the government hosting more consultations at some of the major security research and Internet freedom conferences, with a host of representatives from different government agencies. More overt representatives from the human rights community must be invited to these discussions at all, including the highest, levels.

With regard to the immediate task of implementing the two controls in the United States, I recommend two parallel tracks. The first track is reviewing the language of the two controls and exploring how the language could be improved in a process involving the human rights community, the cybersecurity community, as well as industry. Following Secretary Pritzker's letter, it is now clear that at least part of the language of the two controls will be reviewed by Wassenaar.

However, this is likely to encounter several challenges, including the tradeoff between keeping the language that's fairly broad, but can take into account future technological developments, and therefore without a need of having to be updated soon, compared to narrowing the language and therefore the scope of the control, but requiring the revisions sooner than the broader language. The former requires more trust in the government not to abuse to the broad language for stricter implementation policies. Also, major revisions of the language are not really feasible, given that the majority of the Wassenaar membership has not only agreed, but already implemented the new controls in their national frameworks. And these are only two of many items that are discussed at Wassenaar every year.

The second track would focus on how to implement and develop a licensing policy for the language to apply only to those technologies sold by companies to specific end users in countries with known human rights problems. This will require a nuanced approach, combining the technology-focused controls with the existing or potentially new country charts that Department of Commerce is already using for other export control items. This also needs to include developing FAQs to be issued by the U.S. Government to clarify its interpretation of the language. In terms of the process, it is important to include industry, the cybersecurity research, and human rights community for all parties to develop a shared understanding of the interpretation of the language and implementation.

One option for implementing the two controls more narrowly, in addition to taking into account others' recommendations about possibility exemptions, will be only for exports of technologies to countries with systemic human rights violations. Only these exports would be subject to review or approval or denial by the U.S. Government, with a presumption of denial policy in place for those countries with empirical data of past human rights violations involving such technologies. Export of technologies that fall under the two controls to other countries will only trigger a notification requirement, providing

details about the export—type of product, customer, et cetera—to the government to increase transparency, but will not be subject to the approval regime.

At the multilateral level, it's become clear that while the 41 member states agreed to the same language in December 2013, the implementation of the actual controls and national frameworks has varied widely. Therefore, it is necessary for the U.S. Government to work with other Wassenaar members based on the data that is now becoming available, to ensure that the implementation of the new controls is consistent across its membership in order for the controls to be effective, and in order for controls not to create competitive disadvantage. And in my written statement, you will find some examples of what countries and specific companies this refers to.

The U.S. Government should also collaborate with countries that are not members of the Wassenaar Arrangement, but that focus on building an industry in this area, for example India, to engage them early on in building a broad regime with common standards. One country particularly worth paying attention to in this context is Israel. Israel is not a member of the Wassenaar Arrangement, yet implements Wassenaar controls voluntarily. Israel is therefore also implementing the two new controls—in fact, has even broadened the language. This is particularly noteworthy given Israel's significant cybersecurity industry, the Israeli Government's having made growing this industry a national priority, and the unique security threats Israel is facing. The government's approach to implement the new control is likely to provide further insight into how to strike an appropriate balance between these various interests.

Export controls are only one mechanism in the toolkit to effectively address the underlying human rights problem. They will need to be part of the mix, but we also need to consider other tools—for example, corporate self-regulation and corporate social responsibility. And a voluntary approach driven by industry could include sharing best practices for implementing the know-your-customer practices, to raise the standard across industry. This also includes becoming a member and active participant in industry groups focusing on the intersection of business and human rights, such as the Global Network Initiative, and working with human rights NGOs and research organizations, like EFF, The Citizen Lab, Privacy International, or New America's Open Technology Institute to increase transparency to help name and shame.

Another option would be to consider expanding the GHRAVITY executive order. In April 2012, the Obama administration issued an executive order to address the provision of technologies to Iran and Syria that can be used for surveillance. Expanding the GHRAVITY executive order would be another potential avenue to pursue, but does not have the same type of regime and consultative processes in place that the export control regime already has.

Looking ahead—these are my concluding remarks—it will be important to make these new controls meaningful and effective. Otherwise, governments could rely on other existing controls, namely encryption controls, as a substitute to address the unresolved, underlying human rights problem. This is noteworthy given that another objective of many civil society and industry actors is the further liberalization of encryption controls in the future. Further liberalizing encryption controls will become a lot more complicated and harder to disentangle if encryption controls will also be used to protect human rights in the future.

Relatedly, if encryption controls will be used as a substitute for an effective implementation of these two new controls, some companies might start developing prod-

ucts without encryption automatically being built into them to avoid export controls that might—and technologies that might still be of concern from a human rights perspective. In short, we have yet to address the underlying human rights problem, and it's likely to get worse than better if action is not taken soon.

Thank you, and I look forward to your questions.

Ms. HAN. Great. Thanks, Tim. I want to go back in a minute to talk about one of your proposals about using the human rights controls—country-by-country controls on that, because that's something that's in the Global Online Freedom Act. But first, I'm going to ask a broader question. And just so the audience knows, we will have a chance for people in the audience to ask questions. I'm going to start off asking a few questions, but then others will be able to ask. If you have a burning question, or want to think of a burning question, please do so.

I want to talk about the issue of Balkanization of the Internet. I think this has been touched on a little bit, in the sense that because governments are feeling threatened by information that's coming from all the interaction that Rebecca mentioned between users around the world, we've seen a movement toward countries looking to put up walls around their Internet. China specifically, but also we've seen it in a lot of other places as well. And I think there's been more interest in doing so as potential technologies become available to make that more possible. I think a few years ago people kind of laughed at the idea of it, but as I mentioned before, China's paved the way for a lot of other countries in creating the technologies and the mechanisms to do that.

I want to talk about the issue of that, and what does it mean for U.S. companies who have traditionally been the companies that run the Internet, or have the most stake in—the largest companies, basically. What does that mean for U.S. companies and their operations? What does that mean for people in these other countries that will be behind firewalls?

And Tim, you mentioned the whole idea of encryption and how that could also become—it's always been an issue, but how it's going to continue to be an issue, with the role of encryption in possibly either creating or breaking through those walls. So maybe if each of you could address it from your own perspectives, that would be great.

Ms. MACKINNON. I'm happy to start. I know both the other speakers have some strong expertise on that as well. But as you alluded to, sort of what we call the Balkanization of the Internet is happening really from different motivations coming from different types of governments.You have governments like the Chinese Government, really championing the idea of Internet sovereignty, that sovereign governments have the right to impose whatever rules they want on the Internet within their borders. And so you've seen increasingly strict rules coming from China, but also coming out of Russia as well, requiring that companies host data inside the borders if they want to serve customers in that country, and comply with law enforcement requests and requirements in that country, in order to even access that market.

But you're also seeing from a number of democratic countries other motivations that sort of have a Balkanizing effect. There's a lot of concern, particularly in the wake of the Snowden revelations, about a country's population being vulnerable to surveillance from other governments, and wanting to have more control over the data and privacy of their own citizens, and discussing requirements for multinational companies to host user data within their own borders if they want to service those markets. The motivation of feeling

that they're operating in the public interest by doing that, but posing some serious problems in terms of multinational Internet companies actually being able to service a global user base who want to communicate with one another across borders, and doing so in a way that doesn't just result in making it harder for cross-border communications, and making it harder for cross-border innovation and small companies to actually reach global audiences.

And so this is a new challenge. And I think it speaks to what Lisl was talking about, about the need for a global coordination around norms that will be based in human rights standards, so that we don't willy-nilly have countries acting in their self-interest. And sometimes, you know, believing that they're acting in the interest of their own public and their own domestic public's rights, in a way that's really going to destroy the value of the Internet commercially, as well as in terms of Internet freedom. And so there's kind of these two different sets of motivations at play that could end up having similar results if we're not careful.

Ms. HAN. Before you all weigh in, could I just note that, for example, Kazakhstan put out a notice that they were going to start requiring security certificates for every website or something to be signed in the country, as an example, similar to what you see in China, where because China has not only the technical capability but a certain amount of power to block so much information, and also essentially to create this walled community. For activists, what are the stakes? And do you think other countries are going to be able to emulate that sort of model?

Ms. MACKINNON. Yeah, that's a good question. I think very few countries—with the exception of, let's say, Russia, really have the internal industry to have domestic versions of Twitter, domestic versions of Facebook and YouTube, so that people really don't feel they need the outside services. Which is one reason why China has been so effective. But you know, Chinese and Russian companies are becoming increasingly global. So you could see a situation where a government says: We're only going to let companies in that want to play by our rules. And you could have a situation where, let's say, the Western companies decline, but the Chinese and Russian companies might be quite willing to do that, because they're doing it at home anyway and have the infrastructure to model it. I mean, you could potentially see that.

And you definitely see that already with hardware around the world, and networking equipment in the developing world, where certain authoritarian governments feel much more comfortable working with Huawei or ZTE rather than Cisco because they can get more of what they want. So that's a potential issue to look out for. But for instance, Iran—they're starting to try and foster some domestic industry, but unlike in China where the CPJ is reporting that Weibo, the Chinese version of Twitter, is really completely under the thumb of the government. And Twitter is blocked. People don't really need it, though, for anything except for political activity, and the government has been successful at thwarting circumvention tools. So that's kind of a troubling model that I think we can see duplicated even if global industries themselves aren't as robust in every single country.

Ms. HAN. So, Lisl, can you talk about what the discussions are within the GNI companies about sort of this rock and hard place that they're coming up against in countries where they definitely want to play a role and be in the market, but they're also being pushed to do things that wouldn't comport with their own human rights standards, or

their own ideals? Some companies may not have those hesitations, but from the GNI perspective what are you seeing?

Ms. BRUNNER. Sure. Just in general, you know, the two challenges that face all of these companies in their global operations are laws that are not consistent with international standards—so, for example, as I mentioned earlier, laws that criminalize support for, glorification of, praise for terrorism in extremely raw terms, which are applied in ways that often target political speech, and government practices that are not consistent with the principles of legality, necessity, and proportionality. So we see some governments, for example, blocking all of YouTube because there's a single video that they determine violates their law.

So in many circumstances companies don't have the prerogative to refuse to comply with a lawful order. But when that law is not consistent with international standards, what do they do? So the GNI and its principles provide them with a framework. And often, we've found that when companies say we have a policy in place, we have human rights impact assessments and due diligence measures in place, that makes a difference. Companies can try to minimize the impact of the demand. They can push back and ask for clarification. They can challenge the demand in court occasionally when that appears to be the most prudent thing to do.

And we found that often, or sometimes, the government doesn't come back when it's asked to clarify the request. Companies often receive requests that don't even comply with that law. And so when they point to a policy, or they point to the presence of stakeholders in their home country who are holding them accountable to these policies, to these principles and say, you know, we need for your request to comply with your law, at the very least, that sends a message to governments.

And it means that those requests are more often consistent with the protection of the right to privacy and to freedom of expression. And again, it minimizes sometimes the impact of those requests. It means they don't come back a second time, or they come back and they're correct. The company can keep track of them, can be transparent with the public. And so that's the standard that we would hope that all ICT companies will want to follow.

Ms. HAN. And can you talk about, are U.S. companies, because of this potential for losing market share in other countries if they don't want to participate in markets where it's increasingly becoming more restrictive, do you think there's a role for trade agreements, either within the WTO or the Trans-Pacific Partnership or TTIP that might be useful? Are companies talking about that, about how we could use -or something that fits more neatly within the trade world, or is there some other way that we could create more international norms?

Ms. BRUNNER. We haven't been discussing the WTO or the TTIP recently at GNI, but the movement toward data localization affects most profoundly the users, who know that by using services that perhaps store their information on servers in the United States or elsewhere, they're subject to more robust privacy protections. And moving those protections impacts their ability to engage in the kind of speech that's critical of the government than they would do otherwise, impacts their feeling when they're communicating privately with others. And it also impacts the small- and medium-sized businesses that might arise and provide services to many different countries, and provide more outlets for global expression.

There are many motives for countries increasingly adopting measures that look like data localization. But one of them is frustration in not being able to get data in a timely manner from U.S. providers when they seek it. And so that's why mutual legal assistance reform is high on our agenda. Reforming that system, you know, both through practical means such as increasing funding to the Department of Justice Office of International Affairs, providing training for law enforcement officials in the United States and abroad, making the system electronic, are simple kind of first steps that we could take, and then taking a broader approach to reforming the international legal framework for mutual legal assistance is, I think, urgently needed in the longer term.

Ms. HAN. That's interesting. The original Global Online Freedom Act in 2007 used the MLAT process as the mechanism for trying to cut down or decrease the opportunity for governments to misuse users' data. It directly related to the Yahoo Shi Tao case in China. But then, because, as you mentioned, there are lot of MLAT process, there are some countries that don't have agreements, but there's some where it's just doesn't function very well. So I think it's useful to look at that process going forward. But it does provide a nice legal framework that is kind of missing right now in how the data's being used.

Tim, if you could talk about encryption, in the context of the Balkanization issue, and where you see discussions in encryption going with Wassenaar or domestically? And then, also, the importance of encryption for security.

Mr. MAURER. So I think encryption is another fascinating example for how this is affecting the debate about the fragmentation. And I think there are a couple of pieces, looking at this from an analytical perspective. One, that not all fragmentation or specific actions that are taken are necessarily bad, because the technical experts also sometimes have reasons for localizing data in a specific territory. But that's driven by the technical needs, and not a political motive. And as Rebecca pointed out, this is such a nuanced problem, starting with China and Russia that Rebecca already mentioned, but we've also seen this come up in the context of Brazil. We've also seen this in Germany, where the term technological sovereignty is actually part of the coalition agreement of the current government.

So it's not black and white really anymore. It's a lot more complicated, with countries, including democracies in other countries, that are actively pursuing this, and for very different reasons. The MLAT process is one reason. Encryption is another. And I think as Rebecca pointed out, from a systemic level, either at the root of the current international system's inadequacy to deal with the new technology and data flows. And you can either go the route of trying to internationalize and update those processes like the MLAT process; if that process is not fast enough to keep up with the evolution of the technology, it's not a surprise that countries will default to the sovereignty approach and nationalizing it.

I think it's a very natural reaction. And it'll come down to which of these two different trends is faster. With regards to encryption, I think you have all of these pieces come together, but the trend of the technology has been that encryption is going to be increasingly a big risk. There's a reason why the U.S. Government decided in the 1990s to remove encryption from the munitions control list, and moved it over to the dual use list. And now with the Apple case it's clear that encryption will continue to be, I think, more widely available. And both industry players, as well as human rights organizations, are pushing for further liberalization.

And I think, also talking to people in government agencies and the technical experts, there is only so much you can do with regard to an overarching technological trend. So in terms of looking at some of the older techniques in terms of law enforcement methods that are more reliant upon human intelligence and informants, I think, are things that we ought to be looking into. And the Wassenaar Arrangement, at a very general level, raises another question: To what extent encryption controls, or also the two new controls that were created specifically for technology that can be used for surveillance, ought to be part of that regime that was created to deal with arms during the Cold War, or whether we should be looking into a new regime that specifically deals with digital technologies and with the transfer of these technologies.

Ms. HAN. Yes, you had mentioned in your statement about the issue ofthe human rights aspect of these controls, and that the U.S. already has a crime control regime which is under the dual-use export controls, which gets at items that can be used for torture. This was back—I think it was the early 1990s, the U.S. decided that we didn't want to be exporting instruments of torture to certain governments who might use them against their own citizens. So there's this country chart which specifies where they can't go. And there's an X—we can't send thumbscrews to Indonesia, or something like that.

And so what the Global Online Freedom Act does is also create this new country chart for items that could be used for surveillance or—you know, essentially equating some of these surveillance and censorship tools as similar to instruments of torture. Obviously, you can't equate them, but it's basically, in a simplistic term, using them in that way. The Wassenaar Arrangement came somewhat close to that, but because Wassenaar really only gets at national security controls, the Commerce Department didn't go that extra step and create what we would call a human rights control for them, even though ostensibly the reason for having them controlled is that, I think.

Could you just comment on whether it would be simpler to do what we have, to just create a country chart and say, OK, these items—which some of them really do have actual good uses, which is why most items are on the commerce control list, because they're dual use. They actually have a legitimate commercial use. But they also could be used for nefarious purposes. So if we just created basically a human rights control for these items, do you think that would get around some of the issues that have been raised over the past year with the new rule, or new regulation?

Mr. MAURER. Yes and no. I think we are right now at a point with the letter where it's kind of like a reset and we're going back to four years ago. The reason why I'm not quite sure that that will happen is because this has not been very much in the debate and the hearings about the export control. That in addition to the human rights angle, there's actually a significant interest from the national security community within government to also have these two new controls, because they're—as you said, and I wasn't involved in this, certainly involved in this three years ago—the initial impetus for this was the human rights concern that remains unaddressed.

But what then happened is that professionals of the national security community also noticed that a lot of these products that have been used for spying on citizens in certain countries, these products can be used to hack and actually be used to undermine cybersecurity. So this is why this is such a complicated problem and you have a lot of the cybersecurity industry being very concerned about the impact of this on their own cybersecurity products, and testing software, and other technologies that given the broad

interpretation of the language might now be swept under the consumer controls, are necessary for cybersecurity.

But some of the products that we're concerned with, and the very companies that have exported them to countries where they've been used to violate human rights, could actually be used to undermine cybersecurity. And that piece of the argument—that has been somewhat missing. And I think it is an important reason. So going down the route of using the crime controls of just the human rights aspect I think would be right to address one of the problems of this, but might not necessarily address some of the others.

And maintaining the flexibility by, I think, trying to use first a country-based chart, as pointed out in GOFA, and new lists specifically to the human rights concerns. But then using the notification requirements strategically to gain more data about the type of products and where they're going to I think will be helpful to then refine the regime further down the road. But I think what has become clear in the last year is that the process was not set up. And having to go back to this now, after everything that happened this year, would be even more challenging than three years ago.

Ms. HAN. So just one more clarification, then I'm going to open it up for questions from the audience. You mentioned that some of the other members of Wassenaar have already implemented that rule. Is Italy one of them? [Laughter.] And can you talk about Hacking Team exports, I think, to Egypt that recently came into the news.

Mr. MAURER. Hacking Team is a company based in Italy that was one of the companies that's been most in the news as an example of a company based in a democratic country that has been exporting a product to countries where it's been used for human rights violations. Italy has implemented the new controls, but as Cheri McGuire actually pointed out in her hearing as one of the reasons why the industry's so concerned about this, is the way Italy implemented the control was that it implemented it very broadly, and essentially still allowed Hacking Team to continue to operate its business.

The very reason why these controls were created, from a human rights perspective, and one of the companies it was meant to apply to, the government that's responsible for it now decided to implement the control in a way that it actually is no longer effective. And that's a problem. And I think Cheri McGuire is very right to point to that it's not just about adopting an agreement to the language. It's also important to then have a uniform sense of how are you actually implementing it.

And one more note, because I think this is an interesting insight. An employee of Hacking Team responded to an email I sent when I was writing an article for Slate at one point. And the question was to what extent companies like Hacking Team still have control over their product once it's been sold to a customer. And once a human rights violation becomes known, to what extent they have an ability to still have any influence over the customer. And the response by the employee of Hacking Team was—and he was OK with my publishing this—was that once the product is sold, the company still provides service to keep the product up to date, et cetera, as part of the contract.

So once you find the human rights violation, technically the company still has an ability to then actually terminate that relationship and also take effect in terms of disabling the product, if there is that mechanism to do so. But I thought that was interesting, because it shows, again, like export controls can actually be an interesting tool if they're narrowly tailored and have an impact on human rights.

Ms. HAN. Great, thank you. OK, I'm now going to open it up for questions from the audience. Jacob has a microphone, so raise your hand, and if you could identify yourself. Yes, Alex.

Q: Hi. I'm a journalist from Azerbaijan. I want to ask a question related to Azerbaijan. Azerbaijan is a country where there is an Internet, but there is no freedom. How to protect Internet freedom in Azerbaijan? There is lots of talk about how much they provide access to Facebook. But there's also self-censorship that, you know, people—they keep arresting people for their posts, and that creates another problem. And so how to address that self-censorship in dictatorships? Thank you.

Ms. HAN. That's a great question. And I think it's also interesting that in Azerbaijan the telecommunications infrastructure is owned by the president's family. So even though they may allow Facebook, or allow Gmail, et cetera, they basically have access to everything. Rebecca, you want to start?

Ms. MACKINNON. Sure. I mean, it's really difficult. And actually, related to the telecommunications infrastructure, a Swedish company, TeliaSonera, came under fire for its presence in Azerbaijan——

Ms. HAN. And Uzbekistan.

Ms. MACKINNON. ——and Uzbekistan, and the kind of assistance that the company might have been compelled to give. And it's my understanding they're sort of winding down their businesses in those areas for a number of reasons, including some of these concerns. But then you're just left with the state-owned telecommunications companies. So it's tough. If the government is criminalizing online speech, there's a real question, you know, so what can people outside of that country do, other than sort of support groups outside of the country who are trying somehow to get alternative information in, and to support strong encryption so that people in such countries can actually communicate and evade surveillance, and make themselves more secure.

But it's really tough. And this is a trend we're seeing all over the world, attacks on civil society, and not just online but also offline, just the criminalization of civil society, cutting off of their funding, the increasing squeeze on any kind of independent journalism in a range of countries. And so this is why it's just really incredibly important for democratic countries to stand up for consistent application of laws, to set the example of what a human rights-compatible legal regime looks like, what human rights-compatible corporate practices look like, what an accountable technology kind of ecosystem looks like that's human rights compatible.

If we don't set the right example in democracies, it's going to be harder and harder for people in places like Azerbaijan and many other countries to point to a model of where the country needs to go. A lot of these governments are saying, well, you know, all these other democracies are doing the same thing in different ways. And obviously it's not equivalent if you don't have rule of law or independent press, but nonetheless we're not doing a good enough job at providing models that people around the world can advocate for. And we need to do a better job.

Ms. HAN. Lisl, can you talk about how companies view working in countries like Azerbaijan, where there may ostensibly be very little censorship, and the typical programs—you know, Facebook, Twitter, et cetera, are available in those countries, but in practice you could say that there's very little Internet freedom. What you say online or

what you—even when you communicate what you think is privately, is potentially viewable to the government. So how are companies looking at that?

Ms. BRUNNER. Sure. And I'll just add to Rebecca's point. I think the GNI sees that the Freedom Online Coalition is kind of a positive step in the direction of democracies setting standards for Internet freedom around the world. We'd like to see the Freedom Online Coalition make more progress in this regard, perhaps create some model laws that other countries can implement, perhaps be more of a spokesperson for global Internet freedom in concrete ways.

Yes, we've worked with TeliaSonera over the past few years, which was present in Azerbaijan and many of the countries in that region. And it is definitely a challenging situation. You know, it's important to have a human rights policy, to have a clear procedure in place, to train your employees on what that policy is so that they have a basis for interacting with government officials. The company has taken quite a few measures towards transparency, or trying to be as transparent as possible about its interactions with the government. In the end, as Rebecca mentioned, for a variety of reasons it has determined that withdrawal from that region is the best plan, for other reasons as well.

And that is, I think, a decision that we can respect. At the same time, who's going to go into Azerbaijan once they leave? And is that going to be a win for human rights, if that's a company that does not have a human rights policy, that is not in constant communication with its stakeholders, with its government, with those who champion Internet freedom?

Ms. HAN. OK. Any other questions from the audience? Yes.

Q: Hi. Steven Rashtushen [ph], House Foreign Affairs Committee, Asia-Pacific Subcommittee.

My question is about how specifically with the Wassenaar Arrangement countries could implement certain ways to ensure that certain data has to be in the United States or other countries that would uphold human rights, such as Adobe or Microsoft changing their services, rather than selling technology, licensing it out. Is there a possible way that corporations and government would be amenable to having certain of these services based in countries that they control, and potentially police these human rights violations?

Ms. HAN. Tim, go first, or . . . ?

Mr. MAURER. To be honest, I don't have the insight to be able to answer that question. I'd give you more details but, I don't.

Ms. MACKINNON. I'd be happy to address it a little bit. We've seen quite a lot of instances, particularly with companies—you know, there are a number of companies, including U.S. companies, that store most if not all of their user data in the United States, particularly somewhat smaller companies that have large user bases. Or chose from their data centers, you know, actually kind of do some evaluation in where to put data centers.

What we're finding, though, is sometimes even with companies whose data is outside of a particular jurisdiction, if they have any employees in that jurisdiction then the problem isn't solved. So it's not just a matter of where the data is, it's what are your other vulnerabilities. One case in point is with Facebook and what's happening in Brazil. A Facebook executive was jailed for about 24 hours—fortunately he was released after a higher judge kind of decided it was ridiculous.

But it was because WhatsApp, which is now owned by Facebook, wouldn't hand over user data in a drug investigation case. WhatsApp—not only do they not host data in Brazil anyway, but they have rolled out end-to-end encryption. And so WhatsApp, the company, didn't have access to the data even in the United States. You know, it's just not physically possible to hand over that data.

But then countries are still trying to find ways to basically coerce companies. Or they'll just say, if you don't comply with our request, we're going to block you completely from our market. And so you see a lot of cases where the data is hosted doesn't solve the entire problem.

It can help in some circumstances, particularly with the most oppressive situations—for instance, with the user data in China, if it's physically in China there's no way you can refuse to hand it over, whereas there might be -if it's not in China, there are ways to avoid doing that. But it doesn't go the whole way, particularly in markets like Brazil, which are democracies, which are countries that these companies feel they need to be in, they need to have staff. But then they get coerced in really strange ways. So it's tough.

Ms. HAN. Any more questions? Yes.

Q: I'm an intern from China, so I have experience with what you're saying just now. So it is true that we cannot use Facebook, Google, or Twitter, or other social media in China, because I think—because our government cannot control those companies. So, for example, if I post something or express my opinion online, on the policies of our government, I will be banned, or my opinion will be deleted online.

I think—you know, the most important reason for this phenomenon is because our Chinese Government is not very confident of its democracy, and it's afraid that people in China will be influenced by democratic awareness in the Western countries, which may, you know, overthrow the Chinese Government. But the Chinese market is a very profitable market because China has an enormous population. I wonder whether those companies like Facebook, Google, they will compromise their principles and seek collaboration with Chinese Government, or do you have some specific or detailed ideas or suggestions that can pressure the Chinese Government to change its rules or regulations?

Ms. HAN. That's a really great question. Rebecca, you want to start?

Ms. MACKINNON. Sure. And Lisl can talk about some of the principles that GNI member companies apply. But more broadly, I mean, it's my opinion—just because I've spent some time in China and looking at the Chinese Internet over the years—I've sort of concluded that it's going to be difficult to get—I think foreigners trying to convince the Chinese Government to change is not going to be very successful, for lots of reasons.

I tend to feel that we're only going to see change when Chinese companies themselves begin to view their own commercial interests as different from—basically that complying with censorship and surveillance in a blanket way hurts their business. If Chinese companies become more global, they might need to actually demonstrate to users, if they're trying to grow their user base around the world, that they're upholding some principles. And if we eventually do see a little bit more distance between the interests of Chinese companies and the interests of the government, maybe that's where we might end up seeing a bit of change.

But it's been my observation generally with these issues around the world, when you get a change of law in a positive direction, or when you get a change of policy in a positive direction, or if a bad law is stopped, or sort of a bad practice is stopped, usually it's

because there's some kind of coalition that forms between civil society, in the case of Internet sort of user groups and so on, and some part of industry, and then some part of government that actually ends up seeing it in their interest to move in that direction.

So in some countries there might be some part of the government that really cares about global science and technology, or something. And there might be some politicians who see it in their long-term political interest to advocate a particular position, and ally themselves in that way. But you know, I think China right now is a long way from seeing that. But I think if we're really going to see a sea change in terms of how the government and companies work together, it's going to have to come from within China. There's going to have to be some kind of alliance of interests. And it's going to take a long time.

But we certainly have seen—Google used to have a censored searched engine in China because they wanted the business. They pulled out. Facebook is still blocked in China. They still haven't gone in. What they're going to do in the future it's hard to know. Other companies have made other choices. You know, Microsoft is in China pretty extensively. There are many non-GNI companies that are in China quite extensively, including Apple.

And you know, different companies, I think, are—you know, there are sometimes also situations where there's no perfect choice in terms of what the user's interest is. And so sometimes companies end up having to weigh a number of different options, none of which are great, and choose between sort of least-bad solutions. Because I do think that if companies sort of just refuse to engage anywhere and provide any service anywhere unless there's a policy environment that's perfect—I don't think that's going to be good for the world's Internet users either. So it is a complex picture. But Lisl can talk more.

Ms. HAN. Just let me just further clarify what I'd like for you to talk to, just if you don't mind. This whole issue of what a company's motivation is, either for market share or reputation, they're kind of constantly balancing this. And what is a company's motivation to care about transparency, or to care about—it usually has to come from users—you know, their consumer base, right? It very rarely is something internal to the company.

You know, Google started out with "don't be evil." [Laughter.] But I think they've kind of lost their way on that one. But with Apple, talking about that motivation, certainly in this case that we see right now, I think what their motivation in fighting this case is, they're worried about security. They're worried about the security of their data and their users. I don't think they have really any compunction against helping the FBI get information. I don't think that's an issue. This is more a fundamental security issue for them and their product.

This doesn't apply to Android phones, because it's a completely different business model. So I think it would be interesting to talk about why do companies like Facebook make decisions whether or not to go in, and their brand. If we go back to right after 1989, Levi Strauss famously pulled out of manufacturing in China because it hurt their brand. Here's an American jean company that was—they weren't going to be made by prison labor in China. But they eventually made the decision to go back even though labor issues in China hadn't necessarily changed.

So if you could talk to motivation, and do you think that a lot of the companies in GNI, are they—is this really a user-generated need for them to do this, or what's their motivation for going into a market or not?

Ms. BRUNNER. Well, that's a complex question, the motivation for going into a market. I mean, I think it's difficult to be a global information and communications technology company and exclude a billion users in China and millions of users elsewhere. I think, yes, with the GNI companies and many Western companies, it's the desire of the users to be part of a company with service that is transparent that operates in a way that is consistent with the U.N. guiding principles on business and human rights. And as Rebecca said, the GNI framework is meant not only to apply to companies doing business in easy situations, but to give them some tools for doing business in difficult situations—and in the most difficult situations.

So the principles and the implementation guidelines dealing with specific requests, the types of actions that companies can take. They can say, please clarify this request and tell us exactly where in your law it gives you the authority to ask for this. It allows them to go back to requests and say, actually, we interpret the law differently and we don't think that you need all of that data, you just need this little part of the data. The human rights due diligence process is to ask questions such as, is the way that we can modify this product, or introduce a different product that will enhance privacy or add extra privacy protections?

And then just being able to discuss these opportunities, these options with people like Rebecca MacKinnon, who's an expert in China and other organizations that have contacts on the ground there, that have expertise in these different areas, is incredibly valuable. And that's something that will support our companies as they make these decisions.

Ms. HAN. We have time for one more question, if anybody wants to ask something?

OK, I just want to wrap up and ask sort of a 30,000-foot question. Where do you think we go from here? Because we're kind of at the hard spot right now, I think, with where the Internet is going, where online freedom is going. And it seems like it's moving to where the telecom sector is or has been for a long time, whatever the governments want them to do, they do. But I think that there's still space and there's still so much innovation that's happening within the Internet industry that we still have opportunities. So I'm just wondering if each of you could talk about where you think we might be going in your respective areas.

Lisl, you want to start? Or, Tim, you're ready? OK.

Mr. MAURER. So with regard to the export control issue, I think what we've seen in the last year, and even the discussion since 2013 is only the beginning of this, because I think, both from the human rights perspective, but also from the cybersecurity, national security perspective, this was kind of more of a wake-up call that export controls might be a useful tool. And there's now a much greater sensitively and awareness around it, which will hopefully translate into a more productive process, where we can actually find some language and then an implementation policy that's sensible to what is being—[inaudible]. But mine is—I would guess that this was just the beginning, and these two controls might not be limited to also only what we see in this space.

Ms. BRUNNER. I can speak from the perspective of the GNI. In many ways, we've kind of come out of version 1.0, which was consolidating the organization, conducting the first round of assessments. And now that we've learned those lessons, I think we're in version 2.0, which is taking the lessons from those assessments and translating them into public conversations, into policy engagement, promoting things such as the distribution of alternative messages, rather than the restriction of content when things like terrorist content,

glorification of terrorism are used to try and restrict content, and promoting solutions such as mutual legal assistance as alternatives to things like data liberalization mandates. And as we can, kind of take those practical lessons and get those messages out to the right people, I think that will advance the debate.

Ms. MACKINNON. I think, as I was saying before, we need policy leadership. We need the United States to lead. We need the democratic world to lead. We need to see commitments that, yes, the democratic world is facing some real challenges with terror and use by terrorists of the technologies. But we need to understand that and say, this is a hard problem. Knee-jerk solutions, short-term solutions are not, in the long run, going to solve the problem or make us more secure. And we need to subject our policy solutions to a broader assessment of what is their global human rights impact, what is their impact on the ability of the Internet to be free and open and secure for all of its users, and really subject policy measures and proposals to that kind of test.

And to see coordination amongst democratic governments about building best practices, to be creative on policy solutions around cross-border law enforcement and how trade rules and sanctions are meant to work or not work. I think with the Freedom Online Coalition, I would love to see to the extent possible if Congress can kind of push to see more accountability amongst the Freedom Online Coalition governments. You know, the United Nations has something called the Universal Periodic Review, where governments—on human rights—where governments report to the Human Rights Council on what they're doing to protect human rights in their countries.

I would like to see some reporting coming from the members of the Freedom Online Coalition of what have these governments done to advance online freedom around the world—not just made commitments. And there are some good things—like, there's a fund to support human rights defenders in some of the most problematic countries. But what are democratic governments doing to really exercise policy leadership on the planet right now, and to see evidence of that and to see a plan for doing that, and coordinating on counter terror, law enforcement, and all these kinds of things. And to the extent we can push to have that happen, I think it would be really helpful.

I think that the Global Network Initiative has added real value, and I think made a real difference. And there may not be perhaps enough public understanding of the extent to which it's made a difference with some of the world's most powerful Internet companies. And we do need accountability frameworks. And we have seen over the past 50 years, accountability frameworks around labor standards, around environmental standards. They have really emerged through a combination of legislation, but also from investors stepping up and applying standards to companies, and asking questions of corporate boards. And we're just starting to develop what the standards should be to evaluate Internet and telecommunications human rights practices that can give investors some levers.

We need companies to be sort of reporting more on what it is they are doing. We need greater transparency, a greater commitment, and greater mechanisms to hold them accountable. I think there may be some cases where law can help. There are other cases where the issues are so complex that it might be hard to legislate, but there are a number of, I think, initiatives that can be supported, taking place in the private sector and civil society to really strengthen accountability. I know the Global Online Freedom Act and its evolution over time has examined different approaches to requiring company reporting.

There is a question of should it be to the Security and Exchange Commission, or maybe the FTC that might have more expertise on this to evaluate company disclosure.

I do think that providing leadership is important, and recognizing that this is really a global problem, and a global issue, and setting standards for how companies need to handle their relationships with governments, how they need to treat their users, you know, and making those truly global standards is important.

And Congress has a role to play. I think the executive branch has a role to play in providing leadership on this. I think the private sector, civil society, academia, just the need for more research in terms of cause and effect and what's going on, and what is effective and what's not in terms of interventions is really important, because I think sometimes with some of the funding that goes towards efforts, we're not quite sure what's effective and what's not, so it's really good to have more evaluation of that as well.

I think the good news is, having worked in this space for the past 10 years, is that 10 years ago there weren't that many people working on these issues. And I remember being here on the Hill, in, what was it, like 2006, when a number of companies were called in to explain themselves and their practices in China. And the language they used was quite appalling. It was sort of like, "well, there's nothing we can do" kind of language. You don't hear that anymore.

You hear a very different tone, a very different set of commitments. The discourse around these issues got much more sophisticated. I think there's an understanding of the role everybody needs to play. I think there's now a community working on these issues that didn't exist, with the exception of a few small groups, 10 years ago. And that's really thanks to the leadership in Congress and elsewhere in the government supporting the growth of this community, continuing to shine a light on these issues, continuing to make global Internet freedom part of U.S. policy. No matter how imperfect it is, it's an important pillar of U.S. policy. That needs to be continued and needs to be supported.

So, I kind of want to end on an optimistic note. Despite the tough problems we face out there, and the individuals who are really facing threats, we've seen a lot of progress in terms of the work that's being done. And it would be a lot worse if this community of different stakeholders—government, private sector, NGOs, academics—hadn't stepped up.

Ms. HAN. And a lot of that is thanks to you, Rebecca, because from starting the GNI, and now doing Ranking Digital Rights, you've been the trailblazer in that. So thank you for doing it. And thank you for being here. Tim, thank you. Lisl, thank you. I appreciate everyone for being here. And we're adjourned. [Applause.]

[Whereupon, at 11:35 a.m., the briefing ended.]

APPENDIX

PREPARED STATEMENT OF LISL BRUNNER

Chairman Smith, Co-Chairman Wicker and Members of the U.S. Helsinki Commission, thank you for the opportunity to provide an overview of the Global Network Initiative and its policy priorities.

The Global Network Initiative is an international, multi-stakeholder collaboration between information and communications technology (ICT) companies, civil society organizations, investors, and academics. Formed in 2008, our mission is to promote human rights by creating a global standard for companies that supports responsible decision-making, and by being a leading voice in policy debates to advance freedom of expression and privacy rights in the ICT sector.

The GNI's company members are Facebook, Google, LinkedIn, Microsoft, and Yahoo, and its non-company members include the Berkman Center for Internet & Society, the Center for Democracy and Technology, Human Rights Watch, Bolo Bhi of Pakistan, the Centre for Internet & Society of India, and the Church of Sweden, among many others.[1] For the past three years, the GNI has collaborated with companies participating in the Telecommunications Industry Dialogue. Seven of these global companies recently became observers to the GNI with an aim to become full members in March of next year.

The GNI works in four areas:

1) It provides a framework for responsible company decision-making and action;

2) It fosters accountability through company commitment to an independent assessment process to evaluate their implementation of the Principles;

3) It promotes policy engagement; and

4) It enables shared learning among our participants.

Responsible company decision-making

In the first area, the GNI's Principles and Implementation Guidelines were developed through a multi-stakeholder process and are based on international human rights standards.[2] Our guidelines are influenced by, and are compatible with, the UN Guiding Principles on Business and Human Rights and the 'Protect, Respect, and Remedy' framework. The GNI framework helps member companies to respect and protect the freedom of expression and privacy rights of their customers and users when they respond to government demands, laws and regulations. Companies worldwide can use this framework to implement their responsibility to respect human rights.

Accountability

---

[1] A complete list of participants is available at http://globalnetworkinitiative.org/participants/index.php.

[2] The GNI Principles and Implementation Guidelines are available at http://globalnetworkinitiative.org/corecommitments/index.php.

In terms of accountability, GNI member companies undergo a biennial assessment of their implementation of the GNI Principles, conducted by organizations that are accredited by the GNI's multi-stakeholder Board and which meet independence and competency criteria. In addition to reviewing the GNI company's policies and procedures and interviewing staff members, the assessor selects case studies that determine how a company has responded to government demands involving freedom of expression and privacy. The assessor prepares a report that is reviewed by the GNI Board, and the Board determines whether the companies are complying with the Principles, which means that in the Board's view, the company is making a good faith effort to implement and apply the GNI Principles and to improve over time.

In 2013, the GNI completed assessments for its three founding companies,[3] and its second round of assessments for all member companies is currently underway. The experiences shared through the assessment process are channeled into shared learning and policy efforts.

Policy engagement

In terms of policy engagement, the multi-stakeholder nature of GNI gives us a deep capacity for informed and credible engagement with governments, intergovernmental organizations and international institutions. The GNI generally advocates for laws that are consistent with international human rights standards and with the principles of legality, necessity, and proportionality. At present, we are focusing our policy efforts on five issues of priority.

First, the GNI is concerned by the adoption of broad laws prohibiting extremist content and the promotion of terrorism. The GNI acknowledges the legitimate national security and law enforcement obligations of governments. At the same time, there continues to be no internationally agreed upon definition of terrorism, and across the world, counter-terrorism laws have led to the criminalization of speech in political contexts and to the restriction of large amounts of content in countries like Tajikistan. Similarly, some authorities have proposed that ICT companies should face criminal liability for failing to delete content praising terrorism from their platforms.[4]

This is related to a second area of policy priority, which is legislation on intermediary liability and calls for service providers to police user content and communications, at times under broad and vague standards of what content is considered illegal.

Third, the GNI advocates for laws that regulate government access to user data in a way that protects the right to privacy. Recently, for example, we have engaged with the U.K. government and provided input to consultations on its Investigatory Powers Bill.[5]

---

[3] The Global Network Initiative, Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo (January 2014), available at: http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf

[4] See, The Global Network Initiative, Extremist Content and the ICT Sector: Launching a GNI Policy Dialogue (July 2015), available at: http://globalnetworkinitiative.org/sites/default/files/Extremist%20Content%20and%20the%20ICT%20Sector.pdf.

[5] Global Network Initiative, Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill, December 21, 2015, available at: http://globalnetworkinitiative.org/sites/default/files/Written%20evidence%20- %20Global%20Network%20Initiative.pdf.

The GNI has also urged governments to support strong encryption and not to subvert security standards.[6]

Fourth, the GNI has advocated for reforms to the Mutual Legal Assistance (MLA) regime, which is the dominant method for managing lawful government-to-government requests for data across jurisdictions. The regime has not been updated to keep pace with globalized data, making the process inefficient and opaque, and requests to the U.S. government take an average of 10 months to fulfill. As a result, authorities from other governments sometimes resort to drastic measures. Some states have attempted to demand that their domestic laws apply extraterritorially, have proposed data localization measures, and have sought to compromise the digital security of individuals. All of these measures would be harmful to an open, robust, and free Internet.

The GNI has identified a series of practical and legal reforms that policymakers could adopt in order to reform the current MLA system.[7] We also support efforts to develop a new international legal framework to enable foreign law enforcement authorities to have efficient access to information when this access is consistent with international norms on human rights and privacy. The GNI supports reforms that would allow governments to make requests for data from providers, as long as stringent human rights requirements apply and the process is characterized by robust transparency, accountability, and international credibility.

Finally, the GNI has advocated for governments to take steps to be more transparent about the laws and legal interpretations that authorize electronic surveillance or content removal. Similarly, we urge governments and intergovernmental organizations to take a multistakeholder approach when debating laws and policies that impact the freedom of expression and privacy of Internet users globally and to ensure that these are subject to public debate.[8]

Learning

In terms of learning, the GNI provides opportunities for its members to work through complex issues with other participants in a safe, confidential space. We have commissioned reports that examine the challenges facing governments and technology companies as they balance the rights to freedom of expression and privacy with law enforcement and national security responsibilities. And we have held public learning forums to discuss these challenges in the United States, Brussels, and Geneva.

Conclusion

In conclusion, I would like to highlight a few of the GNI's achievements. The GNI's independent assessment process has yielded tangible changes and improvements in company policies and practices. These include the adoption of human rights impact assessments and the development of enhanced company transparency with customers, users and the wider public. The application of GNI Principles has reduced the amount of content

---

[6] Global Network Initiative, Submission to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (February 2015), available at: http://globalnetworkinitiative.org/sites/default/files/GNI%20Submission%20on%20Encryption.pdf.

[7] Andrew K. Woods, Data Beyond Borders: Mutual Legal Assistance in the Internet Age, The Global Network Initiative (January 2015), available at: https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

[8] See, e.g., Global Network Initiative, Submission to the Office of the UN High Commissioner for Human Rights on "The Right to Privacy in the Digital Age" (April 1, 2014), available at: http://globalnetworkinitiative.org/sites/default/files/GNI%20submission%20OHCHR%20April%201%202014.pdf

removed and personal data released as a result of government requests. We have also successfully encouraged governments to increase transparency and public debate around their surveillance laws, policies and practices, securing commitments on judicial oversight from the almost 30 governments in the Freedom Online Coalition and reforms of surveillance and intermediary liability laws.

Thank you again for the opportunity to give an overview of the GNI and its activities.

The Global Network Initiative is an international multi-stakeholder organization that brings together information and communications technology companies, civil society (including human rights and press freedom groups), academics and investors to work together to forge a common approach to protecting and advancing free expression and privacy around the world. GNI members commit to, and are independently assessed on GNI principles and guidelines for responding to government requests that could harm the freedom of expression and privacy rights of users.

For media inquires, please contact Kath Cummins, kcummins@globalnetworkinitiative.org.

Prepared Statement of Tim Maurer

Chairman Smith, Co-chairman Wicker, Members of the Commission,

It is an honor to testify before you today. Thank you for the opportunity to address the important issue of the role of export controls and internet freedom.

I am an associate at the Carnegie Endowment for International Peace, where I co-lead Carnegie's Cyber Policy Initiative. For the last six years I have been working at the intersection of human rights, cybersecurity, and internet governance. I currently serve as a member of the Freedom Online Coalition's cybersecurity working group "An Internet Free and Secure," am a member of the Research Advisory Network of the Global Commission on Internet Governance.

Export controls are among the most complicated policy issues to address. Export controls combine law, technology, and policy with national- and international-level implications and in this case also sit directly at the intersection of human rights, security, and business. Striking the right balance between benefits and costs is a common challenge across all export control categories for dual-use items. This is especially difficult in the context of new technologies and emerging markets which still lack comprehensive empirical data.

In December 2013, the 41 member states of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies agreed to create two new export controls focusing on "cybersecurity items."[1] he proposed implementation of these two new controls by the U.S. government sparked significant controversy last year and touch on four dimensions that are important to consider:

- Growing empirical evidence of technologies sold by companies in North America and Europe to customers in countries that use them to violate human rights
- The benefit of these technologies for legitimate law enforcement and intelligence activities
- The benefit of these technologies for cybersecurity, for example, to test and improve defenses
- The risks of these technologies for cybersecurity, for example, by providing more sophisticated hacking tools to actors who will use them for offensive purposes

My remarks will focus on the first of these four dimensions, controlling exports of technologies that can be used to violate human rights in the context of Internet Freedom, given the focus of this briefing but each of them raises important questions and challenges worth exploring further. In addition to the substantive considerations, process is another important factor to consider. The controversy over the past year and the significant pushback against the U.S. government's proposed implementation of the two new controls are signs that processes need to be improved. Only two days ago, Secretary Pritzker announced in a letter that

> "In response to these concerns. . .the United States has proposed in this year's Wassenaar Arrangement to eliminate the controls on technology required for the development of 'intrusion software'. We will also continue discussions both domestically and at Wassenaar aimed at resolving the serious scope and implementation issues raised by the cybersecurity community concerning remaining controls and hardware tools for the command and delivery of 'intrusion software.'"

As we enter this new phase in this discussion following Secretary Pritzker's letter, it is helpful to start by looking back at the original problem that led to these new controls. This is worth highlighting because this history and underlying human rights problem were occasionally lost in the controversy over the past year and has yet to be addressed. It is also worth noting that export controls are only one mechanism among a variety of tools to effectively address this first dimension but an important one which is why this briefing is particularly timely.

Introduction: The Emergence of a Difficult Problem

The driving force originally pushing for updated export controls were human rights groups who had grown increasingly concerned [2] that repressive governments were using new technologies to spy on their citizens.[3] These new technologies can be used for different purposes and have been sold on an emerging and growing market. This market first entered into the spotlight after the 2011 Arab uprisings; when the archives of fallen Arab regimes opened to the public, they provided a unique insight into those regimes' inner workings and trade relationships. This included shedding light on companies in North America and Europe who had exported technologies to security and intelligence agencies in countries ranging from Muammar Gadhafi's Libya [4] to Bahrain.[5] In 2011, the *Wall Street Journal* published a catalog [6] shedding light on this burgeoning industry.

One particularly prominent example of the type of company and products that have been at the center of this debate is Hacking Team, an Italy-based company selling technologies designed to access computer networks and collect data. On July 5, 2015, Hacking Team was hacked. The intruder not only changed the firm's Twitter account to "Hacked Team" but exposed some 400Gb of proprietary data to the public. Subsequent media analysis shed light on Hacking Team's client relationships with security agencies in more than 20 countries, including some with dubious human rights records such as Sudan.[7] Another example illustrates that certain governments use these technologies not only within their own borders. A federal court in Washington is currently weighing a lawsuit [8] alleging that the Ethiopian government remotely spied on a U.S. citizen in Maryland. To do so, the Ethiopian government used commercial internet-based technology sold by Gamma International, a company based in the United Kingdom and Germany. This activity was discovered not by the U.S. government, but by Citizen Lab, an academic research center based at the Munk School of Global Affairs at the University of Toronto.

These news reports and research publications also revealed that existing export control regulations did not cover some of the technologies of concern to human rights advocates. Therefore, the French [9] and British governments, which were both particularly criticized for allowing the export of technologies to authoritarian governments that eventually used them for surveillance, each submitted a proposal to amend the list of the Wassenaar Arrangement leading to the adoption of two new controls by its full membership in December 2013.

Background: Wassenaar Arrangement

The creation of these two new controls set a precedent by adding a human rights component to the Wassenaar Arrangement. The stated mission of the Wassenaar Arrangement is "to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations." [10] Unlike its predecessor, the Cold War-era Coordinating Committee for Multilateral Export Controls

(COCOM), the Wassenaar Arrangement does not target any state or group of states, nor can members exercise veto power over other members' export decisions. Rather, the arrangement aims to create a framework for harmonizing national approaches to export controls and to offer a forum for information-sharing.[11]

In December 2013, Wassenaar signatories, including the United States, the member states of the European Union, Japan, and Russia, reached a consensus on adding the two new aforementioned export controls focusing on "intrusion software" and "IP network surveillance systems" to the arrangement's list of regulated technologies. These are technologies used to gain access and to monitor data. Some [12] have described this addition as an attempt to bring "cyberweapons" into the fold of international arms-control agreements and the U.S. government would later describe them as "cybersecurity items." [13]

Because the Wassennaar Arrangement is voluntary and nonbinding, it has no direct effect on national or international law; states must integrate its terms into their respective national frameworks for controlling exports. Over the nearly two years since the passage of the 2013 amendments, the 41 signatory states have focused on implementing the change. So far, implementation across these 41 states remains uneven and while the majority of the membership including Japan and the member states of the European Union implemented the new controls, implementation by the U.S. has been lagging behind.

Analysis of Post-2013 Events and Proposed Implementation in the United States

Because the Wassenaar Arrangement is updated annually, its signatories have generally well-established mechanisms to implement any amendments, and the United States is no exception. Usually the U.S. interagency process takes six months to implement changes agreed to in the multilateral Wassenaar dual-use-technologies export-control list given the consultative process with industry beforehand through the Department of Commerce's Technical Advisory Committees.[14] However, this time it took until May 2015, nearly three times longer than usual, for the U.S. government to publish its decision through the Department of Commerce's Bureau of Industry and Security.

This long delay occurred for two reasons. First, there was a prolonged interagency discussion about the implementation of these two new controls. The outcome was not, as it usually is, a final rule but a proposed rule, which enabled the public to provide feedback during a two-month period. This was unusual and an encouraging demonstration of the government's willingness to engage the public. In fact, Secretary Pritzker's letter now states that this practice will become institutionalized and a standard mechanism moving forward, a decision to be applauded. This can produce more effective outcomes in the future and help build trust among the actors involved, as long as it is used to meaningfully engage in dialogue rather than used to block action.

The second reason for the delay was that despite the administration's long internal deliberations, the proposed rule for implementing the new controls met with stiff resistance from major multinational companies as well as from members of the cybersecurity research community once it was made public. During the subsequent two-month public comment period following the publication of the proposed rule, many businesses, industry groups, and security researchers argued that the bureau's proposal interpreted the Wassenaar language too broadly, echoing more general concern over the wording the Wassenaar Arrangement itself. Companies including Google,[15] Cisco and Symantec,[16] and firms under the umbrella Coalition for Responsible Cybersecurity [17] organized against the

government's formulation. They expressed concern about the potential cost to the industry, the potential effect of slowing down cybersecurity information sharing, and the uneven implementation of the new controls across the Wassenaar membership. Even some of the civil society organizations who had been advocating for an update of export controls [18] voiced concern about the possible effects of the changes and broad language on cybersecurity research offering specific recommendations for how to narrow and tailor their implementation.

The reaction made clear that addressing the problem and updating the export-control regime would be complicated for both historical and technical reasons. Historically, much of this debate is reminiscent of the heated discussions around the Computer Fraud and Abuse Act (CFAA) and encryption controls, known as the "Crypto Wars" of the 1990s, which left scars and entrenched positions among those involved. Moreover, in several cases over the past two decades, federal prosecutors stretching the law's language have used the CFAA to pursue harsh court sentences.[19] Cybersecurity researchers worry that an overly vague or broad regulation could be similarly used in the future. It is therefore no surprise that the U.S. government's proposed implementation of the new controls resurfaced old grievances and revealed significant levels of mistrust among some of the actors involved.

Moreover, the proposed rule exceeded the original language of the 2013 amendment to the Wassenaar Arrangement. That wording had focused more narrowly on network-surveillance systems and intrusion software that is usually developed by companies for sale to governments, not by individual researchers. By contrast, the U.S. proposal outlines a policy of "presumptive denial" and is therefore inclined to deny rather than approve exports and specifically references "zero-day exploits," the vulnerabilities in software that remain undetected and have been known for zero days. Cyber researchers often seek out such vulnerabilities to test a system's security and to alert developers to weaknesses. There are also so-called bug bounty programs and an active market where such vulnerabilities are traded. As the Electronic Frontier Foundation [20] argues, "the only difference between an academic proof of concept and a 0-day for sale is the existence of a price tag." The concern is that the new regulations could have a chilling effect on researchers fearful of being found in violation of the letter of the law, even though their objective is the exact opposite. Department of Commerce representatives have stated [21] that the proposed controls are not intended to limit security research or even the legal trade in zero-day vulnerabilities, but critics worry that such a chilling effect will occur.

As a result of this feedback, the Department of Commerce, in an unusual departure [22] from its normal implementation process, first indicated that it would revise its proposal [23] and eventually the U.S. government followed up with the aforementioned letter by Secretary Pritzker on March 1, 2016.

Moving Forward and Recommendations

It is clear that addressing this problem can only be successful if coordinated multilaterally and informed by technical analysis.[24] Initially, human rights groups expected that the United States would be a leader in implementing these export controls given its prominent Internet Freedom agenda. Now, the United States is part of the minority of countries that have yet to implement the new controls and is reacting to other countries' implementation rather than proactively shaping the standard itself. As others have already observed, the United States is "home to most of the world's cybersecurity companies, holding the number one provider position in the global market—which topped $75

billion in 2015 and could reach $170 billion by 2020." [25] U.S. leadership on this issue and full investment in striking the right balance can therefore have a significant impact and set an example for others. One of the positive outcomes of the controversy of the past several months is a heightened awareness among all actors involved. The underlying human rights problem that led to the development of the new controls has yet to be addressed.

Export controls can be an effective tool to influence corporate behavior.[26] The challenge is designing them so they only target the type of behavior deemed of concern without affecting the rest. Weighing these interests and weighing human rights and security concerns is not a novelty in the context of export controls especially for dual-use technologies.[27] However, this is a new and growing industry with a limited amount of data available therefore making this process more complicated.

Moving forward, I therefore recommend focusing on the following two strategic priorities:

- **Increasing transparency:** a major challenge to addressing this problem effectively and to tailoring export controls accordingly is the lack of information about this market, its players, and the trade of products. Greater transparency can be accomplished through various avenues including voluntary action by companies. In addition, the notification requirements of the export control regime can be a useful mechanism for the government to get a better picture about the market without necessarily imposing a licensing requirement. The data can then be reviewed after a few years to develop a tailored export control regime based on more reliable data.
- **Establishing an efficient and inclusive process:** The controversy of the past year shows that the process to develop, adopt, and implement new export controls needs to be improved. The U.S. government's decision to request public feedback is a promising sign to solicit input beyond the existing standing Technical Advisory Committees. This is particularly important to reach communities such as the cybersecurity research community. A further improvement of the process could consist of the government hosting more consultations at some of the major security research and Internet Freedom conferences composed of representatives from different government agencies. Moreover, representatives from the human rights community must be invited in these discussions at all, including the highest levels.

With regard to the immediate task of implementing the two new controls in the United States, I recommend two parallel tracks:

- A first track reviewing the language of the two new controls and exploring how the language could be improved in a process involving the human rights and security research communities as well as industry.[28] Following Secretary Pritzker's letter, it is now clear that at least part of the language of the two new controls will be reviewed at Wassenaar. However, this process is likely to encounter several challenges including the trade-off between (i) keeping language that's fairly broad but can therefore take into account future technological developments without having to be updated or (ii) narrowing the language and therefore scope of the control but likely to require revisions sooner. The former requires more trust in the government not to use broad language for overly strict implementation policies. At the same time, major revisions to the language are not feasible given that the majority of the Wassenaar membership has not only agreed to but already implemented the new controls and these are only two of many items to be reviewed and discussed overall.

- A second track focusing on how to implement and develop a licensing policy for the language to apply only to those technologies sold by companies to specific end users in countries with known human rights problems. This will require a nuanced approach combining the technology-focused controls with existing or potentially new country charts. This also needs to include developing FAQs to be issued by the U.S. government to clarify its interpretation of the language. In terms of process, it is important to include industry, the cybersecurity research and human rights communities for all parties to develop a shared understanding of the interpretation of adopted language and implementation. One option for implementing the two new controls more narrowly in addition to taking into account others' recommendations [29] about possible exemptions is:
- Only exports of technologies to countries with systemic human rights violations will be subject to a review for approval or denial by the U.S. government with a presumption of denial policy in place for those countries with empirical data of past human rights violations involving such technology [30]
- Export of technologies that fall under the two controls to other countries will only trigger a notification requirement providing details about the export, type of product, customer etc. to the government to increase transparency but will not be subject to an approval review

At the multilateral level, it has become clear that while the 41 member states agreed to the same language in December 2013, implementation of the new controls has varied widely.[31] As Cheri McGuire, vice president for global government affairs & cybersecurity policy at the Symantec Corporation has pointed out in her testimony on January 12, 2016, "[t]he Hacking Team's public business model was to sell offensive intrusion and surveillance capabilities —the exact technology the Wassenaar Arrangement attempted to target with the new controls. However, the Italian export authorities granted a blanket global license to the Hacking Team allowing them to freely export their products around the world to many of the countries that the Wassenaar rule is trying to prevent from obtaining these tools."[32] Moreover, Gamma's actions in Switzerland are a powerful reminder that companies are likely to shop for favorable jurisdictions, and that the global impact of export controls will remain limited without a multilateral regime with uniform and global implementation. Therefore, I recommend:

- the U.S. government to work with other Wassenaar members based on data that is now becoming available to ensure that the implementation of the new controls is consistent across its membership in order for the controls to be effective and in order for the controls not to create a competitive disadvantage.
- the U.S. government to collaborate with countries that are not members of the Wassenaar Arrangement but focus on building an industry in this area, for example, India, to engage them early on in building a broader regime with common standards.

One country particularly worth paying attention to in this context is Israel. Israel is not a member of the Wassenaar Arrangement yet implements Wassenaar controls voluntarily. Israel is therefore also implementing the two new controls, in fact, it has even broadened the language.[33] This is particularly noteworthy given Israel's significant cybersecurity industry, the Israeli government's having made growing this industry a national priority including support from Prime Minister Benjamin Netanyahu at the top,[34] and the unique

security threats Israel is facing. Israel's approach to implementing the new controls is likely to provide further insight into how to strike an appropriate balance between these various interests.

Export controls are only one mechanism in the tool kit to effectively address the underlying human rights issue, as I pointed out at the beginning. They will need to be part of the mix but we also need to consider other tools, namely:

- Corporate self-regulation and corporate social responsibility: The strong reactions from industry have produced a heightened awareness. Translating this heightened awareness into action addressing the underlying human rights problem will require leadership and support from responsible industry leaders to impose peer pressure on industry members with lower standards of due diligence. For example, Jerry Lucas, president of the company that organizes the Intelligence Support Systems conferences that have become known for showcasing surveillance and censorship technology, demurs responsibility. "That's just not my job to determine who's a bad country and who's a good country," he has said. "That's not our business, we're not politicians, we're a for-profit company. Our business is bringing governments together who want to buy this technology." [35] A voluntary approach driven by industry could include
- Sharing best practices for implementing Know-Your-Customer to raise the standard across industry (the Electronic Frontier Foundation has done some groundbreaking work in this area); [36]
- Becoming a member and active participant in industry groups focusing at the intersection of business and human rights such as the Global Network Initiative; [37]
- Working with human rights NGOs and research organizations like EFF, the Citizen Lab, Privacy International, or New America's Open Technology Institute to increase transparency and help name and shame.[38]
- Expansion of "GHRAVITY" executive order: In April 2012, the Obama administration issued *Executive Order Blocking The Property And Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria Via Information Technology* [39] to address the provision of technologies to these two countries that can be used for surveillance. The European Union established [40] a similar ban on exports to Syria. Expanding this "GHRAVITY" [41] Executive Order is another potential avenue to pursue. However, unlike the export control system, this approach has a much less mature system to include and engage with stakeholders outside of government, an issue that will only increase in importance as the technology evolves creating a need to update the language and scope of such regulation. Exploring this option therefore requires particular investment in establishing procedures to engage with and consult experts in industry as well as the cybersecurity research and human rights communities.

Looking ahead, it will be important to make these new controls meaningful and effective. Otherwise, governments could rely on other existing controls, namely encryption controls, as a substitute to address the unresolved underlying human rights problem. Given that another objective of many civil society and industry actors is a further liberalization of encryption controls in the future building on the historic tend, further liberalizing encryption controls will become significantly more complicated and harder to disentangle

if encryption controls will also be used to protect human rights in the future. Relatedly, if encryption controls will be used as a substitute some companies might start developing products without encryption automatically built into them to avoid export controls that might still be of concern from a human rights perspective.

Endnotes

[1] https://www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015-11642.pdf

[2] https://static.newamerica.org/attachments/3936-uncontrolled-global-surveillance-updating-export-controls-to-thedigital-age/Uncontrolled__Surveillance__March__2014.26e1226c08774594bd8a93d5638e8a75.pdf

[3] Parts of this written statement are based on previous publications I have written and co-authored, for example: http://www.worldpoliticsreview.com/authors/1798/tim-maurer http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=182246

[4] http://www.wsj.com/articles/SB10001424053111904199404576538721260166388

[5] http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokiasiemens-networking

[6] http://graphics.wsj.com/surveillance-catalog/

[7] http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech

[8] https://www.eff.org/cases/kidane-v-ethiopia

[9] http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496

[10] http://www.wassenaar.org/introduction/index.html

[11] https://www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015-11642.pdf

[12] http://www.npr.org/sections/alltechconsidered/2015/07/20/424473107/commerce-department-tighter-controlsneeded-for-cyber-weapons

[13] https://www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015-11642.pdf

[14] https://tac.bis.doc.gov/

[15] https://googleonlinesecurity.blogspot.com/2015/07/google-wassenaar-arrangement-and.html

[16] http://passcode.csmonitor.com/wassenaar-comments#chapter-235070

[17] http://www.responsiblecybersecurity.org

[18] https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf

[19] https://www.eff.org/de/issues/cfaa

[20] https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation

[21] http://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200

[22] http://digital-era.net/unusual-re-do-of-us-wassenaar-rules-applauded/

[23] http://www.reuters.com/article/2015/07/29/us-software-exports-regulation-idUSKCN0Q32OQ20150729

[24] http://www.cyberdialogue.ca/2013/03/against-hypocrisy-updating-export-controls-for-the-digital-age-by-daniellekehl-and-tim-maurer/

[25] http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizingand projections. html

[26] Eric Rabe, the chief communications counsel for Hacking Team, provided the interesting insight stating in an email to me that Hacking Team attempts to learn about any possible abuse by vetting clients, monitoring reports of abuses, "require[ing] certain behaviors which we outline in our contract," and "may decided [sic] to suspend support for that client's system rendering it quickly ineffective." His latter comment suggests that it is possible for some products to render such technology ineffective quickly even after the delivery of the system when the customer is found to contribute to human rights violations. See also: http://www.slate.com/articles/technology/future__tense/2014/05/wassenaar__arrangement__u__s__export__control__reform__keeping__surveillance__tech.html

[27] http://www.theguardian.com/world/2012/jul/13/arms-trade-arab-and-middle-east-protests

[28] https://langevin.house.gov/press-release/langevin-statement-obama-administrations-decision-renegotiate-wassenaarintrusion

[29] https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf

[30] An alternative to creating this new list would be selecting or combining existing lists from the Commerce Country Charts: https://www.bis.doc.gov/index.php/forms-documents/doc—view/14-commerce-country-chart

[31] http://www.worldpoliticsreview.com/authors/1798/tim-maurer https://oversight.house.gov/wp-content/uploads/2016/01/McGuire-Symantec-Statement-1-12-Wassenaar.pdf

[32] https://oversight.house.gov/wp-content/uploads/2016/01/McGuire-Symantec-Statement-1-12-Wassenaar.pdf

[33] https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach

[34] http://mfa.gov.il/MFA/InnovativeIsrael/ScienceTech/Pages/PM-Netanyahu-addresses-5th-International-Cybersecurity-Conference-23-Jun-2015.aspx

[35] http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance

[36] https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillanceequipment

[37] https://www.globalnetworkinitiative.org/

[38] Yet, as long as there are companies whose business does not depend on brand reputation and who refuse to follow due diligence with respect to human rights, three is need for a regulatory framework to provide a legal basis for governments to act if necessary.

[39] http://www.whitehouse.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entryunited-states-cer

[40] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:016:0001:0032:EN:PDF

[41] https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20120423—33.aspx

This is an official publication of the **Commission on Security and Cooperation in Europe.**

★ ★ ★

This publication is intended to document developments and trends in participating States of the Organization for Security and Cooperation in Europe (OSCE).

★ ★ ★

★ ★ ★

http://www.csce.gov @HelsinkiComm

The Commission's Web site provides access to the latest press releases and reports, as well as hearings and briefings. Using the Commission's electronic subscription service, readers are able to receive press releases, articles, and other materials by topic or countries of particular interest.

Please subscribe today.